

**REMARKS**

The Office Action received December 4, 2008, has been received and carefully considered. Reconsideration of the current rejections in the present application is respectfully requested based on the following remarks.<sup>1</sup>

I. THE WRITTEN DESCRIPTION REJECTION OF CLAIMS 1 AND 3-11

On page 4 of the Office Action, claims 1 and 3-11 were rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the written description requirement. Further, page 2 of the Office Action (specifically, numbered paragraphs 3 and 4 in the "Response to Arguments" section) addresses Applicant's previous traversal to this rejection. The Office Action states:

3. *Applicant's arguments with respect to the 112 rejections are not persuasive because the specification (page 5, line 15) actually states that "the first and second mask values were equal. Therefore, it is clear that the amendments are wholly unsupported by the specification."*

4. *Applicant has repeatedly chosen to ignore this recitation as pointed to by the Examiner, and has yet to address this recitation.*

---

<sup>1</sup> As Applicant's remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicant's silence as to assertions made by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., assertions regarding dependent claims, whether a reference constitutes prior art, whether references are legally combinable for obviousness purposes) is not a concession by Applicants that such assertions are accurate or such requirements have been met, and Applicant reserves the right to analyze and dispute such in the future.

Applicant would like to specifically respond to these points by referring back to the remarks on pages 9-12 of the previously-submitted Amendment/Response. In these remarks, Applicants points to various portions of the specification that provide support for the allegedly unsupported recitation of "whitening the at least one encrypted message block with a second mask value, which is not identical to the first mask value to generate at least one corresponding output ciphertext block."

From the Examiner's response it does not even appear that these remarks were taken into consideration. Rather, the Examiner simply repeats the position previously taken by pointing to a portion of the specification that is contradictory to the claimed recitation. In so doing, the Examiner is ostensibly applying a standard that has no basis in the patent laws, the patent regulations, judicial opinions, or even the M.P.E.P.

The standard for a written description rejection under 35 U.S.C. § 112(1) is that the patent specification must describe the claimed invention in sufficient detail that one skilled in the art can reasonably conclude that the inventor had possession of the claimed invention. It does not ask whether the inventor

also had possession of different embodiments of the invention that conflicted with a claim element. Indeed, such a rule would effectively abolish the description of alternative embodiments in patent applications.

To illustrate with a hypothetical, imagine a patent application for a lug wrench. Imagine that one portion of the specification describes that the wrench rotates clockwise. Imagine that another portion of the description describes that the wrench rotates counterclockwise. Under the rule that the Examiner appears to be applying, a claim in the hypothetical application that included reference to clockwise rotation would be rejected under 35 U.S.C. § 112(1). A claim that included reference to counterclockwise rotation would also be rejected under 35 U.S.C. § 112(1). By describing alternative embodiments, this hypothetical inventor would have lost the right to claim either embodiment. Quite clearly, this is not what the law requires.

Rather, the standard for 35 U.S.C. § 112(1) is whether the specification reasonably conveys to one skilled in the art that the inventor had possession of the claimed invention at the time the application was filed.

The M.P.E.P. provides some basic guidelines for making this determination (see MPEP 2163). For example, an applicant shows

possession of the claimed invention by describing the claimed invention with all of its limitations using such descriptive means as words, structures, figures, diagrams, and formulas that fully set forth the claimed invention. *Lockwood v. American Airlines, Inc.*, 107 F.3d 1565, 1572, 41 USPQ2d 1961, 1966 (Fed. Cir. 1997). Possession may be shown in a variety of ways including description of an actual reduction to practice, or by showing that the invention was "ready for patenting" such as by the disclosure of drawings or structural chemical formulas that show that the invention was complete, or by describing distinguishing identifying characteristics sufficient to show that the applicant was in possession of the claimed invention. See, e.g., *Pfaff v. Wells Elecs., Inc.*, 525 U.S. 55, 68, 119 S.Ct. 304, 312, 48 USPQ2d 1641, 1647 (1998).

As an additional guideline, the M.P.E.P. states that "[w]hether the specification shows that applicant was in possession of the claimed invention is not a single, simple determination, but rather is a factual determination reached by considering a number of factors. Factors to be considered in determining whether there is sufficient evidence of possession include the level of skill and knowledge in the art, partial structure, physical and/or chemical properties, functional characteristics alone or coupled with a known or disclosed

correlation between structure and function, and the method of making the claimed invention. Disclosure of any combination of such identifying characteristics that distinguish the claimed invention from other materials and would lead one of skill in the art to the conclusion that the applicant was in possession of the claimed species is sufficient." (See MPEP 2163).

With these principles in mind, this rejection is again hereby respectfully traversed.

The Examiner asserts that the claim element "whitening the at least one encrypted message block with a second mask value, which is not identical to the first mask value, to generate at least one corresponding output ciphertext block" is not supported by the specification.

In response to this rejection, Applicant previously referred, and here again refers, to page 13, lines 5-13, of Applicant's specification, which recites:

the method 600 employs two masks  $M_1$  and  $M_2$  that are computed (step 610) based on the two last blocks of value  $E$  and vector  $P$ . Referring to Figure 7A, if  $n$  represents the number of plaintext blocks on input, then  $M_1$  and  $M_2$  are computed by applying a XOR function 410 to the corresponding blocks of  $E$  and  $P$  and then applying a SUBST function 420 as follows:

$$\begin{aligned} M_1 &= \text{SUBST}(P_{n+1} \text{ XOR } E_{n+1}) \\ M_2 &= \text{SUBST}(P_{n+2} \text{ XOR } E_{n+2}) \end{aligned}$$

This recitation clearly indicates that the first and second mask values,  $M_1$  and  $M_2$ , respectively, are computed based upon different P and E values. Applicant also refers to, page 10, lines 25-27, of Applicant's specification, which recites:

if  $U_i$  represents the  $i^{\text{th}}$  counter value, then  
the  $i^{\text{th}}$  value of P is computed as follows:  
 $P_i = \text{Encrypt}(K_2, U_i)$ , ( $i = 1, 2, \dots n+2$ )

This recitation clearly indicates that the vector P is computed based upon different counter values U. Further, page 11, lines 17-19, of Applicant's specification, which recites:

the value, E, is derived by encrypted N  
using the block cipher 210 and the key  $K_1$ .  
Thus, E is an extension of key  $K_1$ .

This recitation clearly indicates that the value E is computed based upon different NONCE values N. Further still, claim 1 recites that the first and second keys,  $K_1$  and  $K_2$ , respectively, have different values. Thus, there is clear support in the specification for the first mask value not being identical to the second mask value, as claimed.

In the Office Action, the Examiner responds to the above by asserting that "this argument is not persuasive because although the calculation for the first and second mask values utilize different P and E variables, there is nothing in the specification that explicitly recites that these variables include a different value." (emphasis added).

At this point it should be noted that, as stated in MPEP § 2163.07(a), by disclosing in a patent application a device that inherently performs a function or has a property, operates according to a theory, or has an advantage, a patent application necessarily discloses that function, theory or advantage, even though it says nothing explicit concerning it. The patent application may later be amended to recite the function, theory, or advantage without introducing prohibited new matter. In re Reynolds, 443 F.2d 384 (CCPA 1971), In re Smythe, 480 F. 2d 1376 (CCPA 1973).

Thus, the Examiner's application of 35 U.S.C. § 112(1) is improper. The application does not have to explicitly state that the different variables include a different value. Rather, the standard is whether the specification enables a reasonably skilled artisan to make or use the claimed invention. Here, this standard is clearly met by the disclosure as explained in the above arguments. As has already been stated above, page 10, lines 25-27, of Applicant's specification recites:

if  $U_i$  represents the  $i^{\text{th}}$  counter value, then  
the  $i^{\text{th}}$  value of  $P$  is computed as follows:  
 $P_i = \text{Encrypt}(K_2, U_i), (i = 1, 2, \dots n+2)$

The specification also states, at page 10 lines 19-26, that "each element,  $P_i$ , of the vector  $P$  is computed by executing an AES block cipher 210 with  $K_2$  as the key using a corresponding

unique values,  $U_i$  (wherein  $i = 1$  to  $n+2$ ). A simple technique that generates a sequence of unique values  $U_i$  is to implement an integer counter of a width suitable to the block cipher 210." (emphasis added). This recitation clearly indicates that the vector  $P$  is computed based upon different counter values  $U_i$ , which are unique in value.

In view of the foregoing, it is respectfully requested that the aforementioned 35 U.S.C. § 112(1) rejection of claims 1 and 3-11 be withdrawn.

## II. THE OBVIOUSNESS REJECTION OF CLAIMS 1 AND 3-11

On pages 4-9 of the Office Action, claims 1 and 3-11 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Rogaway ("OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption") in view of Schneier ("Applied Cryptography, Second Edition") in further view of Jutla (U.S. Patent No. 7,093,126). This rejection is hereby respectfully traversed.

At the outset, Applicant would like to specifically respond to points presented in the "Response to Arguments" section in the Office Action, which states:

5. Applicant argues that, "Rogaway does not disclose any function that could be analogized to the presently claimed application of an XOR function to all message blocks of a message." This argument



*is not persuasive because Rogaway discloses that each message blocks is concatenated (Page 5, checksum generation function). The checksum is then XOR'd with Z[m] (Page 5, calculation of value "T").*

Applicant respectfully disagrees that the concatenation operation described in Rogaway meets the claimed recitation of applying a XOR function to all message blocks of a message to compute a XOR-sum. The concatenation described in Rogaway is a different function than the XOR recited in the claim.

6. Applicant alleges, "Any proposed modification to Rogaway would render the teachings of Rogaway unsatisfactory for its intended purpose." This allegation is completely unsupported by any evidence. Nothing that has been presented by Applicant supports their contention that any proposed modification to Rogaway would render the teachings unsatisfactory.

Applicant has carefully reviewed the previous response and is unable to locate the above language. Rather, Applicant argues that the sheer number of modifications to Rogaway that would be required to arrive at the claimed invention would cause Rogaway to deviate from its intended purpose. Applicant then lists examples (i.e. evidence) of how the modifications to Rogaway would cause Rogaway to deviate from its intended purpose (see previous response pgs. 18-19). These examples, that have

been presented by Applicant, show how the purpose of Rogaway would be frustrated in view of the proposed modifications.

7. Utilizing more than one cryptographic key in Rogaway would hardly render the teachings unsatisfactory for its intended purposes. The security benefits of utilizing multiple keys are well recognized by those of ordinary skill in the art. In addition, utilizing more than one cryptographic key does not change the principle operation, because all aspects of the disclosure remain the same with the exception of using different keys for different cryptographic operations.

8. Applicant argues, "any modification away from that single value key frustrates the intended purpose of having the most efficient possible system with modest memory requirements and limited processing capability." This is not persuasive because storing an extra cryptographic key would not frustrate the memory requirements of the disclosed system of Rogaway. Typical block cipher keys are 64 bits in length.

Applicant respectfully disagrees. Rogaway teaches a single key, single value system. For reasons described in more detail in the body of the response below, the introduction of multiple keys frustrates the purpose and principle mode of operation of Rogaway.

9. Applicant argues, "a concatenation operation is very different from an XOR operation in both form and result." In response, Applicant has misinterpreted the application of the reference. The summation of the XOR is meant to read on the

*claimed concatenation. The Examiner never stated that the XOR operation itself was intended to meet the claimed concatenation, but instead said that it was the XOR-sum.*

The Examiners response in paragraph 9 does not make sense. The claims do not recite a "concatenation" operation and thus it is unclear to Applicant what the Examiner is trying to convey in this response. Further, this response appears to be inconsistent with the response in numbered paragraph 4, which does analogize an XOR function with a concatenation.

*10. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references.*

Applicant does not agree that the form paragraph included as numbered paragraph #10 above is appropriate in the context of Applicant's responses. In any traversal of an obviousness rejection, the references have to be referred to individually at some point along the way. Applicant, though, has carefully argued that the deficiencies of the various combinations of teachings - not merely a single teaching - are what render the rejection improper.

Under 35 U.S.C. § 103, the Patent Office bears the burden of establishing a prima facie case of obviousness. In re Fine, 837 F.2d 1071, 1074 (Fed. Cir. 1988). There are four separate factual inquiries to consider in making an obviousness determination: (1) the scope and content of the prior art; (2) the level of ordinary skill in the field of the invention; (3) the differences between the claimed invention and the prior art; and (4) the existence of any objective evidence, or "secondary considerations," of non-obviousness. Graham v. John Deere Co., 383 U.S. 1, 17-18 (1966); see also KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727 (2007). An "expansive and flexible approach" should be applied when determining obviousness based on a combination of prior art references. KSR, 127 S. Ct. at 1739. However, a claimed invention combining multiple known elements is not rendered obvious simply because each element was known independently in the prior art. Id. at 1741. Rather, there must still be some "reason that would have prompted" a person of ordinary skill in the art to combine the elements in the specific way that he or she did. Id.; In re Icon Health & Fitness, Inc., 496 F.3d 1374, 1380 (Fed. Cir. 2007). Also, modification of a prior art reference may be obvious only if

there exists a reason that would have prompted a person of ordinary skill to make the change. KSR, 127 S. Ct. at 1740-41.

Regarding claim 1, the Examiner acknowledges that Rogaway fails to disclose: 1.) first and second keys having different values to encrypt at least one whitened message block and two other separate values to compute first and second mask values, as claimed; 2.) applying a substitution function to compute first and second mask values, as claimed; 3.) whitening unencrypted and encrypted message blocks using first and second mask values that are different, as claimed. However, the Examiner then asserts that the claimed invention would have been obvious in view of Rogaway, Schneier, and Jutla. Applicant respectfully disagrees. Specifically, Applicant respectfully submits that Rogaway and the other cited references, taken either alone or in combination, fail to disclose, or even suggest, a parallelizable integrity-aware encryption method comprising:

- applying a XOR function to all message blocks of a message to compute a XOR-sum;
- whitening at least one message block with a *first mask value*;
- encrypting the at least one whitened message block using a block cipher and a first key; and
- whitening the at least one encrypted message block with a *second mask value*, which is not identical to the first mask value, to generate at least one corresponding output ciphertext block;
- wherein the *first mask value* is computed by applying a XOR function to a first value derived from

a NONCE value and a second value derived from encrypting a third value using the block cipher and a second key, and then applying a substitution function to the result of the XOR function;

wherein the first and second key have different values;

wherein the *second mask value* is computed by applying a XOR function to a fourth value derived from the NONCE value and a fifth value derived from encrypting a sixth value using the block cipher and the second key, and then applying the substitution function to the result of the XOR function. (emphasis added)

Applicant respectfully submits that Rogaway fails to teach, or even suggest, a first mask value or a second mask value as recited in claim 1. The generated value in the Rogaway XOR operations alleged by the Examiner to be equivalent to the two claimed whitening operations is the same in both operations. This is quite different from a first mask value and a second mask value that are not identical in value as recited in claim 1.

Further, Applicant respectfully submits that Rogaway and the other cited references, taken either alone or in combination, fail to disclose, or even suggest, a parallelizable integrity-aware encryption method that includes, *inter alia*, two keys having different values, as presently claimed. In contrast, Rogaway explicitly discloses using a single key (see Rogaway, pg. 8: "One needs a single key, K, which keys all invocations of the underlying block cipher."). As mentioned

above, the Examiner acknowledges this deficiency of Rogaway (see Office Action, page 5: "Rogaway does not specify that the key used to encrypt the value to generate the 'L' (page 5) is different than the key used to encrypt  $M[i] \oplus Z[i]$  (page 5)."). Neither Schneier nor Jutla cure these deficiencies. Indeed, this is not even alleged. Accordingly, is it respectfully submitted that claim 1 is allowable over the combination of Rogaway, Schneier, and Jutla.

Further, Applicant respectfully submits that Rogaway and the other cited references, taken either alone or in combination, fail to disclose, or even suggest, a parallelizable integrity-aware encryption method that includes, *inter alia*, applying a XOR function to all message blocks of a message to compute a XOR-sum, as presently claimed. Rogaway does not disclose any function that could be analogized to the presently claimed application of an XOR function to all message blocks of a message. Further, Rogaway fails to disclose, or even suggest, any value that could be analogized to the presently claimed XOR-sum.

At this point Applicant would like to respectfully note that, as stated in MPEP § 2143.01, obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some

teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988); In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990). Further, as stated in MPEP § 2143.01, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Additionally, if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. In re Ratti, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

In view of the foregoing, Applicant respectfully submits that it would not have been obvious to one reasonably skilled in the art to modify Rogaway to arrive at the claimed invention. Rogaway is sufficiently different from the claimed invention



that it would not have been obvious to modify Rogaway to arrive at the claimed invention. Claim 1 recites multiple keys. Rogaway only describes the use of a single key. Claim 1 also recites that the multiple keys have different values. Thus, even if the single key of Rogaway was used multiple times, it is substantially different from the claimed invention because it explicitly recites using a single key value. Rogaway also fails to disclose applying a substitution function to compute first and second mask values, and whitening unencrypted and encrypted message blocks using first and second mask values that are different. Claim 1 explicitly recites these features. Thus, it would not have been obvious to one reasonably skilled in the art to modify Rogaway to arrive at the claimed invention.

Also, modifying Rogaway to arrive at the claimed invention would render Rogaway unsatisfactory for its intended purpose. Indeed, the sheer number of modifications to Rogaway that would be required to arrive at the claimed invention would cause Rogaway to deviate from its intended purpose. For example, Rogaway calls for modest memory requirements and limited pre-processing capability (see Rogaway, pg. 8). Rogaway explicitly discloses that the memory requirements and pre-processing capability are only expanded for limited purposes, such as storing  $L(i)$  values. In this discussion, reference is made to

the single key (K). There is no teaching of flexibility with respect to K. Rather, Rogaway reiterates that the key is a single value. Accordingly, any modification away from that single value key frustrates the intended purpose of having the most efficient possible system with modest memory requirements and limited processing capability. Additional modifications with respect to applying a substitution function to compute first and second mask values, and whitening unencrypted and encrypted message blocks using first and second mask values that are different, as recited in claim 1, would only further cause Rogaway to deviate from its intended purpose.

Regarding combining Rogaway with Schneier, such a combination would result in an inoperable methodology since replacing the result of encrypting of Rogaway with an additional XOR function as mentioned by Schneier would not result in a limited tag length  $\tau$ , which is required by Rogaway.

Regarding combining Rogaway with Jutla, such a combination would also result in an inoperable methodology since, first of all, Rogaway fails to even disclose using any mask values, let alone two different mask values, as claimed. Also, Jutla does not explicitly disclose the use of mask values, let alone two different mask values, as claimed. Further, even if Jutla did disclose two different mask values (which it doesn't), using

such two different mask values in Rogaway would not result in a limited tag length  $\tau$ , which is required by Rogaway.

In view of the foregoing, it is respectfully submitted that claim 1 is allowable over the combination of Rogaway, Schneier, and Jutla.

Regarding claims 3-11, these claims are dependent upon independent claim 1. Thus, since independent claim 1 should be allowable as discussed above, claims 3-11 should also be allowable at least by virtue of their dependency on independent claim 1. Moreover, these claims recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

In view of the foregoing, it is respectfully requested that the aforementioned obviousness rejection of claims 1, and 3-11 be withdrawn.

### III. THE OBVIOUSNESS REJECTION OF CLAIMS 12-20

On pages 9-12 of the Office Action, claims 12-20 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Rogaway ("OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption") in view of Schneier ("Applied Cryptography, Second Edition"). This rejection is hereby respectfully traversed.

Regarding claim 12, this claim recites subject matter related to claim 1. Thus, the arguments set forth above with respect to claim 1 are equally applicable to claim 12. Accordingly, it is respectfully submitted that claim 12 is allowable over Rogaway and Schneier for at least the same reasons as set forth above with respect to claim 1.

Also, the Examiner asserts that the claimed invention would have been obvious in view of the combination of Rogaway and Schneier. Applicant respectfully disagrees. The Examiner (see Office Action, pg. 3) alleges that the Rogaway disclosure of concatenating message blocks meets the recited claim 12 element of applying an XOR function to all message blocks of a message to compute an XOR-sum. The Examiner states "concatenation effectively creates the XOR-sum." Applicant disagrees that the concatenation described in Rogaway meets this claim element. A concatenation operation is very different from an XOR operation in both form and result. Applicant respectfully requests withdrawal of the rejection.

Furthermore, Rogaway also discloses applying a string  $L$  and an offset  $Z[m]$  to one string of a message  $M$  before a block cipher  $E_k$ , as well as applying the same message string  $M[m]$  after the block cipher  $E_k$  (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

Additionally, Rogaway also discloses applying an offset  $Z[m]$  to a checksum before a block cipher  $E_k$ , and then limiting the block cipher result to a tag length  $\tau$  (see pages 4-6). This disclosure by Rogaway clearly differs from the claimed invention.

Regarding combining Schneier with Rogaway, such a combination would result in an inoperable methodology since replacing the result of encrypting of Rogaway with an additional XOR function as mentioned by Schneier would not result in a limited tag length  $\tau$ , which is required by Rogaway.

In view of the foregoing, it is respectfully submitted that claim 12 is allowable over the combination of Rogaway and Schneier.

Regarding claims 13-20, these claims are dependent upon independent claim 12. Thus, since independent claim 12 should be allowable as discussed above, claims 13-20 should also be allowable at least by virtue of their dependency on independent claim 12. Moreover, these claims recite additional features which are not disclosed, or even suggested, by the cited references taken either alone or in combination.

In view of the foregoing, it is respectfully requested that the aforementioned obviousness rejection of claims 12-20 be withdrawn.

IV. CONCLUSION

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

To the extent necessary, a petition for an extension of time under 37 CFR § 1.136 is hereby made.

Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-0206, and please credit any excess fees to the same deposit account.

Respectfully submitted,

Hunton & Williams LLP

By: 

Thomas E. Anderson

Registration No. 37,063

TEA/ple

1900 K Street, N.W.  
Washington, D.C. 20006-1109  
Telephone: (202) 955-1500  
Facsimile: (202) 778-2201

Date: March 4, 2009